The tame automorphism group
in two variables
over basic Artinian rings

Joost Berson

Abstract

In a recent paper it has been established that over an Artinian ring R all two-dimensional polynomial automorphisms having Jacobian determinant one are tame if R is a $\mathbb{Q}$-algebra. This is a generalization of the famous Jung-Van der Kulk Theorem, which deals with the case that R is a field (of any characteristic). Here we will show that for tameness over an Artinian ring, the $\mathbb{Q}$-algebra assumption is really needed: we will give, for local Artinian rings with square-zero principal maximal ideal, a complete description of the tame automorphism subgroup. This will lead to an example of a non-tame automorphism, for any characteristic $p > 0$.

Keywords: Affine space; polynomials over commutative rings; group of polynomial automorphisms; group of tame automorphisms

1 Introduction

All two-dimensional polynomial automorphisms over a field are tame, as stated in the famous theorem by Jung and Van der Kulk ([7],[8]). For fields of characteristic zero this was proved by Jung, and Van der Kulk generalized it to arbitrary characteristic. As is well-known, the statement fails to be true over a domain R which is not a field. The most common example of a non-tame automorphism is the one by Nagata ([9]), which is defined over $R = k[Z]$ (a univariate polynomial ring), but can be transformed into an example over any domain which is not a field. For any domain R, [4, Corollary 5.1.6] even yields an algorithm to decide whether or not an automorphism in two variables over R is tame. To continue with the description of the tame automorphism groups over commutative rings in general, it is very convenient to start with Artinian rings. Namely, when it is clear which automorphisms in two variables over Artinian rings are tame, we can use this information to decribe the automorphisms over rings with higher Krull dimension, by lifting the former automorphisms (see for example Theorem 3.4). Moreover, the problem of describing the structure of the automorphism group over a general Artinian ring can be reduced to the case of a local Artinian ring (as will be explained in section 4).

One of the main results of the recent paper [2] by Van den Essen, Wright and the author is the fact that, over an Artinian ring R, all two-dimensional automorphisms with Jacobian

Joost Berson, Radboud University, Faculty of Science, P.O. Box 9010, 6500 GL Nijmegen, The Netherlands, j.berson@science.ru.nl

determinant one are tame in case R is a $\mathbb{Q}$-algebra. This is a generalization of Jung's Theorem. We show that in a non-$\mathbb{Q}$-algebra setting, tameness is not guaranteed. In fact, for every characteristic $p > 0$ we give an example of a non-tame automorphism over a local Artinian ring having that characteristic. To show that these automorphisms are not tame, we provide a description of the structure of the tame automorphism groups over local Artinian rings of the most basic type to be found: the ones with square-zero principal maximal ideal.

This paper is set up as follows: In the next section we introduce the general automorphism group and its best-known subgroups. We describe classic results, explain which questions are still unanswered and in what way this paper contributes to the development of the theory on polynomial automorphism groups. In section 3, we review one of the results of the recent paper [2], saying that over an Artinian $\mathbb{Q}$-algebra R, any two-dimensional automorphism is tame, provided that the Jacobian determinant is equal to one (Theorem 3.5). The preparations for this result, which will be done in that section, are also important for the remainder of this paper: most techniques also work in the non-$\mathbb{Q}$-algebra setting. Lemma 3.1 is in fact the only tool that requires a $\mathbb{Q}$-algebra. Section 4 examines the structure of the elementary automorphism subgroup $\mathrm{EA}_2(R)$ for rings R of the form $R = A[T]/(T^2)$, where A is another ring. It essentially reduces the description of the elementary subgroup over R to the description of the elementary subgroup over A. This result can immediately be applied to the case of local Artinian rings with square-zero principal maximal ideal. This is done in the last section. It yields an example for every prime number p of a non-tame automorphism in two variables over $\mathbb{F}_p[T]/(T^2)$.

2 Automorphism subgroups and their relations

In this paper, every ring is assumed to be commutative and to have an identity element. We will restrict ourselves to polynomial rings in two variables over a ring R, denoted as $R[X, Y]$. This section describes the usual subgroups of the general polynomial automorphism group, and what is already known about how they are related.

A *polynomial map over R* is an ordered pair (F, G) of polynomials of $R[X, Y]$. We can view polynomial maps as maps $R^2 \to R^2$, defined by $(x, y) \mapsto (F(x, y), G(x, y))$, but also as R-endomorphisms $R[X, Y] \to R[X, Y]$, given by the substitution $h(X, Y) \mapsto h(F, G)$. F and G are called the *coordinates* of (F, G).

In the usual notation, the composition of two polynomial maps (F_1, G_1) and (F_2, G_2) is defined as $(F_1, G_1) \circ (F_2, G_2) = (F_1(F_2, G_2), G_1(F_2, G_2))$. The map (F_1, G_1) is called an *invertible polynomial map* or an *automorphism* if there exist a polynomial map (F_2, G_2) with $(F_1, G_1) \circ (F_2, G_2) = (F_2, G_2) \circ (F_1, G_1) = (X, Y)$ (the identity map). The automorphisms form a group, $\mathrm{GA}_2(R)$.

We write $\mathrm{J}\varphi$ for the Jacobian matrix of an automorphism φ. By the chain rule, for any automorphism φ we have $\mathrm{J}\varphi \in \mathrm{GL}_2(R)$, whence $|\mathrm{J}\varphi| \in R[X]^*$. (Throughout this paper, the operator $|\ |$ takes the determinant of a matrix.)

Here is an overview of the usual subgroups of $\mathrm{GA}_2(R)$:

1. $\mathrm{SA}_2(R)$, the *special automorphism group*, is the subgroup of all φ for which $|J\varphi| = 1$.

2. The group $\mathrm{GL}_2(R)$ of invertible matrices is usually viewed as a subgroup of $\mathrm{GA}_2(R)$.

3. $\mathrm{EA}_2(R)$ is the subgroup generated by the elementary automorphisms. An *elementary* automorphism is one of the form $(X + f(Y), Y)$ or $(X, Y + f(X))$ for some univariate polynomial f.
   Note that $\mathrm{EA}_2(R) \subseteq \mathrm{SA}_2(R)$.

4. $\mathrm{TA}_2(R)$, the group of *tame* automorphisms, is the subgroup generated by $\mathrm{GL}_2(R)$ and $\mathrm{EA}_2(R)$.

In the case of a field we have the following classic theorem, which was already mentioned in the introduction.

Theorem 2.1 (Jung [7] - Van der Kulk [8])**.** *For any field k we have $TA_2(k) = GA_2(k)$.*

So over a field the only examples of polynomial automorphisms are the tame ones. However, this doesn't hold for a domain which is not field. But there exists an algorithm to decide whether or not an automorphism in two variables over a domain R is tame in [4, Corollary 5.1.6]). This algorithm can be used to show that any non-unit $r \in R \backslash \{0\}$ produces a non-tame automorphism, namely

$$\left(X - 2Y(rX + Y^2) - r(rX + Y^2)^2, Y + r(rX + Y^2) \right)$$

For a polynomial ring $R = k[Z]$ and $r = Z$, k a field, this is Nagata's famous example ([9]). But for a general commutative ring little is known about which automorphisms in $GA_2(R)$ are tame. This paper is meant to extend our knowledge on this subject.

If $R \to S$ is a surjective ring homomorphism, then the induced group homomorphism $EA_2(R) \to EA_2(S)$ is also surjective. Note that this fails to hold for $TA_2(R) \to TA_2(S)$, because of the following: if $M \in GL_2(S)$, then there doesn't necessarily exist an $N \in GL_2(R)$ such that $N \mapsto M$. This is why tame automorphisms appearing in this paper are usually elements of $EA_2(-)$: we can lift these to automorphisms over rings with higher Krull dimension. Therefore, we would like to know the connection between $TA_2(R)$ and $EA_2(R)$. The following lemma (a special version of [2, Proposition 3.20]) and corollary decribe this connection, which applies to most coefficient rings considered in this paper.

In the following, $SL_2(R)$ denotes the group of all matrices with determinant one, $D_2(R)$ is the group of all invertible diagonal matrices, and $E_2(R)$ is the group generated by all elementary matrices.

Lemma 2.2. *If R is a ring for which $SL_2(R) = E_2(R)$, then $TA_2(R) \cap SA_2(R) = EA_2(R)$. The hypothesis holds when R is a local ring.*

Proof. From $GL_2(R) = \langle SL_2(R), D_2(R) \rangle = \langle E_2(R), D_2(R) \rangle \subseteq \langle EA_2(R), D_2(R) \rangle$ we get that $TA_2(R) = \langle GL_2(R), EA_2(R) \rangle \subseteq \langle D_2(R), EA_2(R) \rangle$, whence $TA_2(R) = \langle D_2(R), EA_2(R) \rangle$. Since one can then readily verify that $EA_2(R) \triangleleft TA_2(R)$, this implies that $TA_2(R) = D_2(R)EA_2(R)$. But then $TA_2(R) \cap SA_2(R) = (D_2(R) \cap SA_2(R))EA_2(R) = (D_2(R) \cap SL_2(R))EA_2(R) = (D_2(R) \cap E_2(R))EA_2(R) \subseteq EA_2(R)$. This proves the first statement.

For the second statement, consider an element M of $SL_2(R)$, where R is local. Since $\det(M) = 1$, there must at least be one entry of M which is in R^*. We can use this entry to clear the other entries of the row and column to which this entry belongs, through multiplication by 2 elementary matrices. If the resulting matrix isn't diagonal, we can make it so by multiplying it with the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in E_2(R)$$

Hence, we may assume that the resulting matrix is diagonal, and since it is still an element of $SL_2(R)$, we can use the fact that, for any ring R and any $a \in R^*$,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in E_2(R)$$

$\square$

Remark 2.3. If R is not assumed to be local, then the hypothesis of Lemma 2.2 still holds if R has a special structure, *e.g.* when R is a Euclidean domain (the proof of this well-known fact is very much like the proof of the second part of Lemma 2.2). It is important to note, however, that

3

not all Principal Ideal Domains have this property. Let R be the ring of integers of $\mathbb{Q}(\sqrt{-19})$, one of the finitely many imaginary quadratic number fields of which the ring of integers is a Principal Ideal Domain, by the Stark-Heegner Theorem ([10], [6]). In [3, Theorem 6.1] it was shown that, if $\alpha := \frac{1}{2} + \frac{1}{2}\sqrt{-19}$, then the following matrix is in $\mathrm{SL}_2(R)$, but not in $\mathrm{E}_2(R)$:

$$\begin{pmatrix} 3 - \alpha & 2 + \alpha \\ -3 - 2\alpha & 5 - 2\alpha \end{pmatrix}$$

Corollary 2.4. *For any ring R we have the following: if $EA_2(R) = SA_2(R)$, then $TA_2(R) = \{\varphi \in GA_2(R) : |J\varphi| \in R^*\}$. The reverse holds if R is any ring for which $SL_2(R) = E_2(R)$.*

Proof. For the first statement, let $\varphi \in \mathrm{GA}_2(R)$ with $|\mathrm{J}\varphi| \in R^*$ (since R is reduced). Then there exists an $\alpha \in \mathrm{GL}_2(R)$ such that $\alpha\varphi \in \mathrm{SA}_2(R) = \mathrm{EA}_2(R)$. Thus, $\varphi \in \mathrm{TA}_2(R)$.

The second statement follows directly from Lemma 2.2. $\qquad\square$

3 The Artinian $\mathbb{Q}$-algebra result

Throughout this section (except for Lemma 3.2), we assume that R is a $\mathbb{Q}$-algebra. We will restate and give a quick proof of one of the results from [2]: for an Artinian $\mathbb{Q}$-algebra R, every special automorphism in two variables over R is tame (Theorem 3.5). The fact that this is also true for any reduced Artinian ring ($\mathbb{Q}$-algebra or not) had already been observed in [9, Corollary 0.6] and [1, Proposition 3.10]. One of the basic tools of Theorem 3.5 is Lemma 3.2. This lemma is also useful for the general (non-$\mathbb{Q}$-algebra) case in the subsequent sections. Lemma 3.1 is taken from [2], and its statement also appeared in [4, § 5.2, Exercise 7]. It is the only ingredient of Theorem 3.5 that requires R to be a $\mathbb{Q}$-algebra.

Lemma 3.1. *Every monomial $X^n Y^m$ in $R[X, Y]$ can be written as a $\mathbb{Q}$-linear combination of polynomials of the form $(X + aY)^{n+m}$, with $a \in \mathbb{Q}$.*

The following lemma also appears (in some form) in [2] and [5] and is a basic property of the type of automorphisms considered in this paper (also over non-$\mathbb{Q}$-algebras).

Lemma 3.2. *Let $\mathfrak{a} \subset R$ be an ideal such that $\mathfrak{a}^2 = (0)$. Suppose $G_1, G_2, H_1, H_2 \in \mathfrak{a}[X, Y]$ are given, and define $\varphi, \psi \in R[X, Y]^2$ by $\varphi = (X + G_1, Y + G_2)$ and $\psi = (X + H_1, Y + H_2)$. Then $\varphi\psi = \psi\varphi = (X + G_1 + H_1, Y + G_2 + H_2)$.*
In particular, $\varphi \in GA_2(R)$ with $\varphi^{-1} = (X - G_1, Y - G_2)$.

Proof. Straightforward. $\qquad\square$

The type of tame automorphisms considered in the following proposition provides a foundation on which we can build many other tame automorphisms.

Proposition 3.3. *Let $\mathfrak{a} \subseteq R$ be an ideal such that $\mathfrak{a}^2 = (0)$. Suppose $\varphi \in SA_2(R)$ has the form $\varphi = (X + g, Y + h)$, where $g, h \in \mathfrak{a}[X, Y]$. Then $\varphi \in EA_2(R)$.*

Proof. Since $\mathfrak{a}^2 = (0)$, $|J(\varphi)| = 1 + \frac{\partial g}{\partial X} + \frac{\partial h}{\partial Y}$. Then $\frac{\partial g}{\partial X} + \frac{\partial h}{\partial Y} = 0$, and since R is a $\mathbb{Q}$-algebra, this implies that there exists a polynomial $p \in \mathfrak{a}[X, Y]$ such that $g = \frac{\partial p}{\partial Y}$ and $h = -\frac{\partial p}{\partial X}$. Using Lemma 3.2, we may assume that $p = rX^n Y^m$ for some $r \in \mathfrak{a}$, $n, m \geq 0$ and $n + m \geq 1$. With Lemma 3.1, we can write $X^n Y^m$ as a $\mathbb{Q}$-linear combination of polynomials of the form $(X + aY)^{n+m}$, with $a \in \mathbb{Q}$. Applying Lemma 3.2 again, we may assume that

$$\varphi = \left(X + kabr(X + aY)^{k-1}, Y - kbr(X + aY)^{k-1} \right)$$

4

where $k = n + m$ and $a, b \in \mathbb{Q}$. But then $\varphi = \alpha^{-1} \beta \alpha$, where $\alpha = (X + aY, Y)$ and $\beta = (X, Y - kbr X^{k-1})$. Therefore $\varphi \in \mathrm{EA}_2(R)$. $\qquad\square$

The following theorem is a special case of [2, Theorem 4.1].

Theorem 3.4. *Let $\mathfrak{a}$ be an ideal contained in the nilradical of R, and $\overline{R} = R/\mathfrak{a}$. Let $\varphi \in SA_2(R)$. If $\overline{\varphi} \in EA_2(\overline{R})$, then $\varphi \in EA_2(R)$.*

Proof. Since the assumption that $\overline{\varphi} \in \mathrm{EA}_2(\overline{R})$ can be expressed using only finitely many coefficients in the ideal $\mathfrak{a}$, we may assume that $\mathfrak{a}$ is finitely generated. Hence it is a nilpotent ideal, say $\mathfrak{a}^m = (0)$ for some $m \geq 1$. We will prove by induction on m that φ is a composition of elementary automorphisms.

The case $m = 1$ is trivial. Now suppose $m \geq 2$ and let $\tilde{R} = R/\mathfrak{a}^{m-1}$ and $\tilde{\mathfrak{a}} = \mathfrak{a}/\mathfrak{a}^{m-1}$. Since $\tilde{\varphi} \in \mathrm{SA}_2(\tilde{R})$, the induction hypothesis (applied to the ring $\tilde{R}$ and its ideal $\tilde{\mathfrak{a}}$) says that $\tilde{\varphi} \in \mathrm{EA}_2(\tilde{R})$. Since $R \to \tilde{R}$ is surjective, we can lift $\tilde{\varphi}$ to a $\varphi_0 \in \mathrm{EA}_2(R)$. Then $\varphi_0^{-1} \varphi = (X + H_1, Y + H_2)$, where $H_1, H_2 \in \mathfrak{a}^{m-1}[X, Y]$. The conclusion $\varphi \in \mathrm{EA}_2(R)$ now follows from Proposition 3.3. $\qquad\square$

Theorem 3.5. *If R is Artinian, then $SA_2(R) = EA_2(R)$.*

Proof. The special case of a field follows from Corollary 2.4 and Theorem 2.1. For the general case, let η be the nilradical of R. Since R is Artinian, it is well-known that R/η is a product of fields. The statement now follows from Theorem 3.4 and the fact that, for any direct product of rings $R = R_1 \times R_2$, the group $\mathrm{EA}_2(R)$ is canonically isomorphic to the direct product of groups $\mathrm{EA}_2(R_1) \times \mathrm{EA}_2(R_2)$. (And the same for $\mathrm{SA}_2(-)$.) $\qquad\square$

4 The square-zero principal ideal setting

To find the structure of the general polynomial automorphism group over an Artinian ring R, we can restrict ourselves to the case of local Artinian rings. Namely, it is well-known that $R \cong R_1 \times R_2 \times \cdots \times R_m$, a direct product of local Artinian rings. And then $\mathrm{GA}_2(R)$ is canonically isomorphic to the direct product of groups $\mathrm{GA}_2(R_1) \times \mathrm{GA}_2(R_2) \times \cdots \times \mathrm{GA}_2(R_m)$. One can readily check that this also holds if $\mathrm{GA}_2(-)$ is replaced by one of its mentioned subgroups.

The remainder of this paper will be focused on the case of a specific type of local Artinian rings, namely the ones for which the maximal ideal is principal and has its square equal to zero. The question of tameness over any Artinian ring can be reduced to this setting. We will see that the automorphism group has a clear structure in this case. To describe the basic aspects of this structure, we can use a more general setting: we suppose (for the moment) that R is any ring containing an element t satisfying $t^2 = 0$. In specific examples, such a ring is usually obtained as a factor ring of a univariate polynomial ring: $R = A[T]/(T^2)$, and $t = T + (T^2)$. We often use the notation $A[t]_2$ to denote this ring. For this kind of ring we will give an explicit description of the group $\mathrm{EA}_2(R)$ in terms of the group $\mathrm{EA}_2(A)$. This will be very useful in the next section, when we apply this to the situation that R is local Artinian.

The conjugation formulas below are crucial properties of the structure of the automorphism group $\mathrm{SA}_2(R)$.

Proposition 4.1. *For any $h \in R[X, Y]$ and $\alpha = (f(X, Y), g(X, Y)) \in SA_2(R)$,*

$$\alpha^{-1}(X + t\tfrac{\partial h}{\partial Y}, Y - t\tfrac{\partial h}{\partial X})\alpha = (X + t\tfrac{\partial}{\partial Y}(h(f,g)), Y - t\tfrac{\partial}{\partial X}(h(f,g)))$$

In particular, if $m \in \mathbb{N}$ satisfies $m + 1 \in R^*$, and $F := \frac{1}{m+1} f^{m+1}$ and $G := \frac{1}{m+1} g^{m+1}$, then

$$\alpha^{-1}(X, Y - tX^m)\alpha = (X + t\tfrac{\partial F}{\partial Y}, Y - t\tfrac{\partial F}{\partial X})$$

5

$$\alpha^{-1}(X + tY^m, Y)\alpha = (X + t\frac{\partial G}{\partial Y}, Y - t\frac{\partial G}{\partial X})$$

Proof. Let $\alpha^{-1} = (p(X,Y), q(X,Y))$. Since $t^2 = 0$, for any $u \in R[X,Y]$ we have

$$u(X + t\frac{\partial h}{\partial Y}, Y - t\frac{\partial h}{\partial X}) = u(X,Y) + t\frac{\partial h}{\partial Y}\frac{\partial u}{\partial X} - t\frac{\partial h}{\partial X}\frac{\partial u}{\partial Y} = u(X,Y) + t|\mathrm{J}(u,h)|$$

Moreover, since $|\mathrm{J}(f,g)| = 1$, the chain rule gives

$$|\mathrm{J}(u(f,g), h(f,g))| = |(\mathrm{J}(u,h))(f,g)||\mathrm{J}(f,g)| = |(\mathrm{J}(u,h))(f,g)|$$

The composition $\alpha^{-1}(X + t\frac{\partial h}{\partial Y}, Y - t\frac{\partial h}{\partial X})\alpha$ can now be written as

$$
\begin{aligned}
\alpha^{-1}(X + t\tfrac{\partial h}{\partial Y}, Y - t\tfrac{\partial h}{\partial X})\alpha
&= (p(X,Y) + t|\mathrm{J}(p,h)|, q(X,Y) + t|\mathrm{J}(q,h)|) \circ (f,g) \\
&= (X + t|(\mathrm{J}(p,h))(f,g)|, Y + t|(\mathrm{J}(q,h))(f,g)|) \\
&= (X + t|\mathrm{J}(p(f,g), h(f,g))|, Y + t|\mathrm{J}(q(f,g), h(f,g))|) \\
&= (X + t|\mathrm{J}(X, h(f,g))|, Y + t|\mathrm{J}(Y, h(f,g))|) \\
&= (X + t\tfrac{\partial}{\partial Y}(h(f,g)), Y - t\tfrac{\partial}{\partial X}(h(f,g)))
\end{aligned}
$$

$\square$

These conjugation formulas naturally inspire us to make the following definition.

Definition 4.2. For any $h \in R[X,Y]$ we define $\varphi^{(h)} \in \mathrm{SA}_2(R)$ by $\varphi^{(h)} := (X + t\frac{\partial h}{\partial Y}, Y - t\frac{\partial h}{\partial X})$.

Remark 4.3. The automorphisms of the form $\varphi^{(h)}$ have the following properties:

1. $\varphi^{(h_1)}\varphi^{(h_2)} = \varphi^{(h_1 + h_2)}$ for any $h_1, h_2 \in R[X,Y]$ (by Lemma 3.2)
2. $\alpha^{-1}\varphi^{(h)}\alpha = \varphi^{(h(f,g))}$ for $\alpha = (f,g) \in \mathrm{SA}_2(R)$ (by Proposition 4.1)

In particular, if $m \in \mathbb{N}^*$ satisfies $m \in R^*$, and if $a \in R$, and $f \in R[X,Y]$ is one of the coordinates of an automorphism $\alpha \in \mathrm{EA}_2(R)$, then $\varphi^{(\frac{a}{m}f^m)} \in \mathrm{EA}_2(R)$. Combining this with property 1. yields many tame automorphisms: if we let $H = \frac{a_1}{m_1}f_1^{m_1} + \cdots + \frac{a_r}{m_r}f_1^{m_1}$, where $a_i \in R$, $m_i \in \mathbb{N}^* \cap R^*$ and each f_i is a coordinate of an automorphism in $\mathrm{EA}_2(R)$, then $\varphi^{(H)} \in \mathrm{EA}_2(R)$. In case $R = A[t]_2$, where the ring A is contained in a $\mathbb{Q}$-algebra, we have a reverse statement, displayed in Theorem 4.6.

In the proof of Theorem 4.6, we use the following group-theoretic lemma.

Lemma 4.4. *Let $G = H \ltimes N$ be a semidirect product of a subgroup H and a normal subgroup N. Suppose we have a subset $S \subseteq N$ such that H and S generate the whole group G. Then $N = \langle h^{-1}sh : h \in H, s \in S \rangle$.*

Proof. First, note that we may replace S by $S \cup S^{-1}$. Now suppose $n \in N$. Then also $n \in G$, so we may write $n = h_1 s_1 \cdots h_r s_r h_{r+1}$ with $h_1, \ldots, h_{r+1} \in H$ and $s_1, \ldots, s_r \in S$ (some of the h_i can be chosen to equal the identity). Viewing this mod N, we obtain $1 = \overline{n} = \overline{h_1}\overline{s_1} \cdots \overline{h_r}\overline{s_r}\overline{h_{r+1}} = \overline{h_1} \cdots \overline{h_{r+1}}$, as $S \subseteq N$. The fact that the composition $H \hookrightarrow G \twoheadrightarrow G/N$ is an isomorphism, gives $1 = h_1 \cdots h_{r+1}$. Using this fact, we can rewrite n as

$$n = (h_1 s_1 h_1^{-1})((h_1 h_2)s_2(h_1 h_2)^{-1}) \cdots ((h_1 \cdots h_r)s_r(h_1 \cdots h_r)^{-1})$$

$\square$

Before we reveal the structure of the group $\mathrm{EA}_2(R)$, we fix a notation for a specific subgroup.

Definition 4.5. $\mathrm{GA}_2(tR)$ denotes the subgroup of $\mathrm{GA}_2(R)$ consisting of those elements that have the form

$$(X + tP(X,Y), Y + tQ(X,Y))$$

with $P,Q \in R[X,Y]$. Furthermore, $\mathrm{EA}_2(tR) := \mathrm{GA}_2(tR) \cap \mathrm{EA}_2(R)$. Note that $\mathrm{GA}_2(tR) = \mathrm{Ker}(\mathrm{GA}_2(R) \to \mathrm{GA}_2(R/tR)) \lhd \mathrm{GA}_2(R)$. Consequently, also $\mathrm{EA}_2(tR) \lhd \mathrm{EA}_2(R)$. Obviously, if R is of the form $R = A[t]_2$, then $\mathrm{GA}_2(tR) = \mathrm{GA}_2(tA)$ and $\mathrm{EA}_2(tR) = \mathrm{EA}_2(tA)$.

Theorem 4.6. *Let A be a ring which is contained in a $\mathbb{Q}$-algebra Q. Let $R := A[t]_2$. Then, for any $\varphi_1 \in \mathrm{EA}_2(R)$, there exist a $\varphi_0 \in \mathrm{EA}_2(A)$ and an $H \in Q[X,Y]$ with $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in A[X,Y]$ such that*

$$\varphi_1 = \varphi_0 \circ \varphi^{(H)} = \varphi_0 \circ (X + t\tfrac{\partial H}{\partial Y}, Y - t\tfrac{\partial H}{\partial X})$$

Moreover,

$$H = \tfrac{a_1}{m_1} f_1^{m_1} + \cdots + \tfrac{a_r}{m_r} f_1^{m_1}$$

where $a_i \in A, m_i \in \mathbb{N}^*$ and each f_i is a coordinate of an automorphism in $\mathrm{EA}_2(A)$.

Proof. Let $\varphi_1 \in \mathrm{EA}_2(R)$. $R = A \oplus At$, so $\mathrm{EA}_2(R) = \langle \mathrm{EA}_2(A), \mathrm{EA}_2(tA) \rangle$. Since we've also seen that $\mathrm{EA}_2(tA) \lhd \mathrm{EA}_2(R)$ and as it is clear that $\mathrm{EA}_2(A) \cap \mathrm{EA}_2(tA) = \{\mathrm{id}\}$, we may conclude that $\mathrm{EA}_2(R) = \mathrm{EA}_2(A) \ltimes \mathrm{EA}_2(tA)$. So, write $\varphi_1 = \varphi_0 \circ \varphi_t$, with $\varphi_0 \in \mathrm{EA}_2(A)$ and $\varphi_t \in \mathrm{EA}_2(tA)$. Now define $S \subseteq \mathrm{EA}_2(tA)$ by

$$S = \{(X + a_i t Y^{m_i}, Y) \,:\, a_i \in A, m_i \in \mathbb{N}\} \cup \{(X, Y - a_i t X^{m_i}) \,:\, a_i \in A, m_i \in \mathbb{N}\}$$

Note that $\langle S \rangle = \{ (X + tP(Y), Y + tQ(X)) \,:\, P(Y) \in R[Y], Q(X) \in R[X] \}$ (the subgroup generated by S), implying that $\langle S \rangle \neq \mathrm{EA}_2(tA)$. For example, $(X + t(X - Y), Y + t(X - Y)) = (X + Y, Y)(X, Y + tX)(X - Y, Y) \in \mathrm{EA}_2(tA)$. However, it is easily seen that $\mathrm{EA}_2(R) = \langle \mathrm{EA}_2(A), S \rangle$. So $G := \mathrm{EA}_2(R), H := \mathrm{EA}_2(A), N := \mathrm{EA}_2(tA)$ and S satisfy the requirements of Lemma 4.4. As a result, we can write

$$\varphi_t = (\tau_1^{-1} \varepsilon_1 \tau_1)(\tau_2^{-1} \varepsilon_2 \tau_2) \cdots (\tau_r^{-1} \varepsilon_r \tau_r)$$

where each $\tau_i \in \mathrm{EA}_2(A)$ and each $\varepsilon_i \in S$ (note that $S^{-1} = S$). Then, using Proposition 4.1,

$$\tau_i^{-1} \varepsilon_i \tau_i = (X + a_i t f_i^{m_i} \tfrac{\partial f_i}{\partial Y}, Y - a_i t f_i^{m_i} \tfrac{\partial f_i}{\partial X}) = (X + t\tfrac{\partial h_i}{\partial Y}, Y - t\tfrac{\partial h_i}{\partial X})$$

for some $f_i \in A[X,Y]$, and where $h_i := \frac{a_i}{m_i + 1} f_i^{m_i + 1} \in Q[X,Y]$. Note that f_i is a coordinate of an automorphism in $\mathrm{EA}_2(A)$. Now we can define $H(X,Y) := h_1 + \cdots + h_r$, and we derive

$$\tau_1^{-1} \varepsilon_1 \tau_1 \cdots \tau_r^{-1} \varepsilon_r \tau_r = (X + t\tfrac{\partial H}{\partial Y}, Y - t\tfrac{\partial H}{\partial X})$$

Obviously, $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in A[X,Y]$, whence φ_1 has the prescribed form. $\qquad\square$

In case the coefficient ring is of the form $B[t]_2$ for a ring B which is *not* contained in a $\mathbb{Q}$-algebra, the above theorem can still be used to unravel the structure of the group $\mathrm{EA}_2(R)$, as is shown in Corollary 4.7.

Corollary 4.7. *Let A be a ring which is contained in a $\mathbb{Q}$-algebra Q. Let $\mathfrak{a} \subseteq A$ be an ideal, and define $B := A/\mathfrak{a}$. Let $R := A[t]_2$ and $\overline{R} := B[t]_2$. Then, for any $\varphi_1 \in \mathrm{EA}_2(\overline{R})$, there exist a $\varphi_0 \in \mathrm{EA}_2(B)$ and an $H \in Q[X,Y]$ with $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in A[X,Y]$ such that*

$$\varphi_1 = \varphi_0 \circ \overline{\varphi^{(H)}} = \varphi_0 \circ (X + t\overline{\tfrac{\partial H}{\partial Y}}, Y - t\overline{\tfrac{\partial H}{\partial X}})$$

Moreover,

$$H = \tfrac{a_1}{m_1} f_1^{m_1} + \cdots + \tfrac{a_r}{m_r} f_1^{m_1}$$

where $a_i \in A, m_i \in \mathbb{N}^*$ and each f_i is one of the coordinates of an automorphism in $\mathrm{EA}_2(A)$.

Proof. Let $\varphi_1 \in \mathrm{EA}_2(\overline{R})$. Obviously, there exists a $\Phi_1 \in \mathrm{EA}_2(R)$ such that $\overline{\Phi_1} = \varphi_1$. The existence of φ_0 and $\varphi^{(H)}$ now follows from Theorem 4.6. $\qquad\square$

5 The case of a local Artinian ring with square-zero principal maximal ideal

In the previous section we examined the structure of $\mathrm{EA}_2(R)$ in the general setting of a ring with a square-zero principal ideal. Now we specialize to the situation that the ring is local Artinian and the ideal is maximal. Whereas every automorphism over an Artinian $\mathbb{Q}$-algebra is tame (Theorem 3.5), this is not true anymore in prime characteristic, as is shown by the following theorem.

Theorem 5.1. *Let p be any prime number and $R = \mathbb{F}_p[t]_2$. Then $SA_2(R) \not\subseteq TA_2(R)$. More precisely, the following automorphism over R is not tame:*

$$(X + tX^p Y^{p-1}, Y)$$

Proof. Suppose $\varphi_1 := (X + tX^p Y^{p-1}, Y)$ is tame. R is a local ring, so $\varphi_1 \in \mathrm{EA}_2(R)$ by Lemma 2.2. Now we can apply Corollary 4.7 with $A := \mathbb{Z}$, $\mathfrak{a} := p\mathbb{Z}$ and $Q := \mathbb{Q}$. Hence, there exists an $H \in \mathbb{Q}[X,Y]$ with $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in \mathbb{Z}[X,Y]$ such that

$$\varphi_1 = (X + t\overline{\tfrac{\partial H}{\partial Y}}, Y - t\overline{\tfrac{\partial H}{\partial X}})$$

(Note that the φ_0 of Corollary 4.7 equals the identity, since $\varphi_1 \in \mathrm{EA}_2(t\mathbb{F}_p)$.) So $\overline{\frac{\partial H}{\partial Y}} = X^p Y^{p-1}$, which implies that the monomial $X^p Y^p$ occurs in $H(X,Y)$, say with coefficient $\frac{a}{b}$, where $a \in \mathbb{Z}\backslash\{0\}$ and $b \in \mathbb{N}^*$ with $\gcd(a,b) = 1$. As $\frac{\partial H}{\partial Y} \in \mathbb{Z}[X,Y]$, also $\frac{pa}{b} X^p Y^{p-1} \in \mathbb{Z}[X,Y]$, whence $b \mid p$ (since $\gcd(a,b) = 1$). Moreover, $\overline{\frac{p}{b}}\,\overline{a} = \overline{\frac{pa}{b}} = 1$, so $a \notin p\mathbb{Z}$ and $b = p$. And $\overline{\frac{\partial}{\partial X} \frac{a}{p} X^p Y^p} = \overline{a} X^{p-1} Y^p \neq 0$. So the monomial $X^{p-1} Y^p$ occurs in $\overline{\frac{\partial H}{\partial X}}$, but this contradicts the fact that $\overline{\frac{\partial H}{\partial X}} = 0$! (since $\varphi_1 = (X + tX^p Y^{p-1}, Y)$) So φ_1 cannot be tame. $\square$

The next example shows, that for $p = 2$, a slightly modified version of the automorphism in Theorem 5.1 is tame. It is unknown to the author if, for all other primes p, the corresponding modified automorphism is tame.

Example 5.2. *Let $R = \mathbb{F}_2[t]_2$. Although $(X + tX^2Y, Y) \in SA_2(R)$ is not tame according to Theorem 5.1, it became apparent at the end of the proof that this is because the monomial XY^2 doesn't occur in the second component of this automorphism. Then the following question arises: is the special automorphism $(X + tX^2Y, Y - tXY^2)$ tame over R? Yes, it is! Since X^2Y and XY^2 are the partial derivatives of $\frac{1}{2}X^2Y^2$ (over $\mathbb{Q}$), we establish the tameness by writing this term as a linear combination of powers, in the style of (the end of) Remark 4.3:*

$$\begin{aligned}
\frac{1}{2}X^2Y^2 \;=\; & \frac{1}{4}(X+Y)^4 - \frac{1}{3}(Y+X^2)^3 + \frac{1}{2}(Y+X^4)^2 - \frac{1}{2}(Y+X^3)^2 - \frac{1}{2}(X+Y^3)^2 \\
& -\frac{1}{2}X^8 + \frac{5}{6}X^6 + \frac{1}{2}Y^6 - \frac{1}{4}X^4 - \frac{1}{4}Y^4 + \frac{1}{3}Y^3 + \frac{1}{2}X^2
\end{aligned}$$

Applying Proposition 4.1 to each of the terms appearing in this linear combination (taking $R = \mathbb{Q}[t]_2$), we get that $(X + tX^2Y, Y - tXY^2)$ equals the composition

$$\varepsilon_0(\alpha_1^{-1}\varepsilon_1\alpha_1)(\alpha_2^{-1}\varepsilon_2\alpha_2)(\alpha_3^{-1}\varepsilon_3\alpha_3)(\alpha_4^{-1}\varepsilon_4\alpha_4)(\alpha_5^{-1}\varepsilon_5\alpha_5)$$

where $\varepsilon_0 = (X + tY^2 - tY^3 + 3tY^5, Y) \circ (X, Y - tX + tX^3 - 5tX^5 + 4tX^7)$ and

$$\begin{aligned}
\alpha_1 &= (X+Y, Y) & \varepsilon_1 &= (X, Y - tX^3) \\
\alpha_2 &= (X, Y + X^2) & \varepsilon_2 &= (X - tY^2, Y) \\
\alpha_3 &= (X, Y + X^4) & \varepsilon_3 &= (X + tY, Y) \\
\alpha_4 &= (X, Y + X^3) & \varepsilon_4 &= (X - tY, Y) \\
\alpha_5 &= (X + Y^3, Y) & \varepsilon_5 &= (X, Y + tX)
\end{aligned}$$

Note that this is actually a composition over $\mathbb{Z}[t]_2$. Viewing this composition over R by calculating modulo 2, we obtain

$$(X + tX^2Y, Y - tXY^2) \in EA_2(R)$$

Let p be a prime number. From Corollary 4.7 it follows that, if $R := \mathbb{Z}[t]_2$ and $\overline{R} := \mathbb{F}_p[t]_2$, then any automorphism in $EA_2(\overline{R})$ is (up to an automorphism in $EA_2(\mathbb{F}_p)$) of the form $\overline{\varphi^{(H)}}$ for some $H \in \mathbb{Q}[X,Y]$ with $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in \mathbb{Z}[X,Y]$. The automorphism $(X + tX^pY^{p-1}, Y) \in SA_2(\overline{R})$ is not of this form (which has been shown in the proof of Theorem 5.1), so it cannot be tame. It is still unknown to the author whether tameness (more precisely: 'being an element of $EA_2(\overline{R})$') is guaranteed for all automorphisms over $\overline{R}$ of the form $\overline{\varphi^{(H)}}$. By Corollary 4.7, this question is equivalent to the following (Question 5.4). A more general version is Question 5.3.

Question 5.3. *Can every $H \in \mathbb{Q}[X,Y]$ with $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in \mathbb{Z}[X,Y]$ be written as a sum of the form $\frac{a_1}{m_1}f_1^{m_1} + \cdots + \frac{a_r}{m_r}f_1^{m_1}$, where $a_i \in \mathbb{Z}, m_i \in \mathbb{N}^*$ and each f_i is one of the coordinates of an automorphism in $EA_2(\mathbb{Z})$?*

Question 5.4. *If the answer to Question 5.3 is negative, let p be a fixed prime number. Does there exist, for every $H \in \mathbb{Q}[X,Y]$ with $\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y} \in \mathbb{Z}[X,Y]$, a sum $H' = \frac{a_1}{m_1}f_1^{m_1} + \cdots + \frac{a_r}{m_r}f_1^{m_1}$ as in Question 5.3, such that $\overline{\frac{\partial H}{\partial X}} = \overline{\frac{\partial H'}{\partial X}}$ and $\overline{\frac{\partial H}{\partial Y}} = \overline{\frac{\partial H'}{\partial Y}}$ in $\mathbb{F}_p[X,Y]$?*

If Question 5.4 also has a negative answer, then the next challenge is to find an algorithm to decide for a given p and H whether such an H' exists. Such an algorithm would thus also be an algorithm for tameness in $SA_2(\mathbb{F}_p[t]_2)$.

We conclude with an example of a monomial $H \in \mathbb{Q}[X,Y]$ which has the property that $\overline{\varphi^{(H)}} \in EA_2(\mathbb{F}_p[t]_2)$ for all primes $p \neq 2$. It is unknown to the author whether this also holds for $p = 2$.

Example 5.5. *It is readily verified that $\frac{2}{3}X^3Y^3 = \sum_{i=1}^{35} h_i$, where*

$h_1 = -\frac{1}{6}(X+Y)^6$ $h_2 = (Y+X^3)^4$ $h_3 = \frac{5}{4}(X+Y^2)^4$ $h_4 = \frac{5}{4}(Y+X^2)^4$ $h_5 = -2(Y+X^6)^3$

$h_6 = -\frac{5}{3}(X+Y^4)^3$ $h_7 = -\frac{5}{3}(Y+X^4)^3$ $h_8 = -\frac{5}{3}(X+Y^3)^3$ $h_9 = -\frac{5}{3}(Y+X^3)^3$ $h_{10} = 3(Y+X^{12})^2$

$h_{11} = -2(Y+X^9)^2$ $h_{12} = \frac{5}{2}(X+Y^8)^2$ $h_{13} = \frac{5}{2}(Y+X^8)^2$ $h_{14} = \frac{1}{2}(X+Y^5)^2$ $h_{15} = \frac{1}{2}(Y+X^5)^2$

$h_{16} = -3X^{24}$	$h_{17} = 4X^{18}$	$h_{18} = -\frac{5}{2}X^{16}$	$h_{19} = -\frac{5}{2}Y^{16}$	$h_{20} = \frac{2}{3}X^{12}$
$h_{21} = \frac{5}{3}Y^{12}$	$h_{22} = -\frac{1}{2}X^{10}$	$h_{23} = -\frac{1}{2}Y^{10}$	$h_{24} = \frac{5}{3}X^9$	$h_{25} = \frac{5}{3}Y^9$
$h_{26} = -\frac{5}{4}X^8$	$h_{27} = -\frac{5}{4}Y^8$	$h_{28} = \frac{1}{6}X^6$	$h_{29} = \frac{1}{6}Y^6$	$h_{30} = -\frac{5}{4}X^4$
$h_{31} = -\frac{9}{4}Y^4$	$h_{32} = \frac{10}{3}X^3$	$h_{33} = \frac{16}{3}Y^3$	$h_{34} = -3X^2$	$h_{35} = -4Y^2$

Note that every $h_i \in \mathbb{Q}[X,Y]$ with $\frac{\partial h_i}{\partial X}, \frac{\partial h_i}{\partial Y} \in \mathbb{Z}[X,Y]$. Now, for every prime $p \neq 2$ we have $\frac{p+1}{3}X^3Y^3 = \sum_{i=1}^{35} \frac{p+1}{2}h_i$, from which it follows (using the same method as in Example 5.2) that $\overline{\varphi^{(\frac{1}{3}X^3Y^3)}} = \overline{\varphi^{(\frac{p+1}{3}X^3Y^3)}} \in EA_2(\mathbb{F}_p[t]_2)$.

References

[1] J. Berson, Two-dimensional stable tameness over Noetherian domains of dimension one, J. Pure and Appl. Algebra 178 (2003) no.2 115-129

[2] J. Berson, A. van den Essen, D. Wright, Stable tameness of two-dimensional polynomial automorphisms over a regular ring, preprint: arXiv:0707.3151v8 [math.AC], submitted to J. Amer. Math. Soc. April 2009

[3] P. Cohn, On the structure of the GL_2 of a ring, Publ. Math. Inst. Hautes Études Sci. 30 (1966) 365-413

[4] A. van den Essen, Polynomial automorphisms and the Jacobian Conjecture, Progress in Mathematics Vol. 190, Birkhäuser, Basel-Boston-Berlin, 2000

[5] A. van den Essen, S. Maubach, S. Vénéreau, The special automorphism group of $R[t]/(t^m)[x_1,\ldots,x_n]$ and coordinates of a subring of $R[t][x_1,\ldots,x_n]$, J. Pure and Appl. Algebra 210 (2007) no.1, 141-146

[6] K. Heegner, Diophantische Analysis und Modulfunktionen, Math. Z. 56 (1952) 227-253

[7] H. Jung, Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math. 184 (1942) 161-174

[8] W. van der Kulk, On polynomial rings in two variables, Nieuw Arch. Wiskd. 3 (1953) no.1 33-41

[9] M. Nagata, On automorphism group of $k[x, y]$, Department of Mathematics, Kyoto University, Lectures in Mathematics, No. 5, Kinokuniya Book-Store Co., Ltd., Tokyo, 1972

[10] H. Stark, A Complete Determination of the Complex Quadratic Fields of Class Number One, Michigan Math. J. 14 (1967) 1-27